VAPT Guide For Penetration Testers - 2023

Vulnerability Management Guide

Table of Contents

I. Introduction

Series Welcome

Welcome to the CRR Resource Guide series. This document is one of 10 resource guides developed by the Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) to help organizations implement practices identified as considerations for improvement during a Cyber Resilience Review (CRR).[1] The CRR is an interview-based assessment that captures an understanding and qualitative measurement of an organization's *operational resilience*, specific to IT operations. Operational resilience is the organization's ability to adapt to risk that affects its core operational capacities.[2] It also highlights the organization's ability to manage operational risks to critical services and associated assets during normal operations and during times of operational stress and crisis. The guides were developed for organizations that have participated in a CRR, but any organization interested in implementing or maturing operational resilience capabilities for critical IT services will find these guides useful.

The 10 domains covered by the CRR Resource Guide series are

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. **Vulnerability Management** ⇦***This guide***
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The objective of the CRR is to allow organizations to measure the performance of fundamental cyber security practices. DHS introduced the CRR in 2011. In 2014, DHS launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). The NIST CSF provides a common taxonomy and mechanism for organizations to

1. describe their current cybersecurity posture
2. describe their target state for cybersecurity
3. identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. assess progress toward the target state
5. communicate among internal and external stakeholders about cybersecurity risk

The CRR Self-Assessment Package includes a correlation of the practices measured in the CRR to criteria of the NIST CSF. An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may fall short of, or exceed, corresponding practices and capabilities in the NIST CSF.

Each resource guide in this series has the same basic structure, but each can be used independently. Each guide focuses on the development of plans and artifacts that support the implementation and execution of operational resilience capabilities. Organizations using more than one resource guide will be able to leverage complementary materials and suggestions to optimize their adoption approach. For example, this guide describes the process of performing a focused and defined vulnerability management process. The development of this process can be informed by the information learned and developed in a controls management process. The outputs of the vulnerability process are key components of a risk management process.

Each guide derives its information from best practices described in a number of sources, but primarily from the CERT®[1] Resilience Management Model (CERT®-RMM).[3] The CERT-RMM is a maturity model for managing and improving operational resilience, developed by the CERT Division of Carnegie Mellon University's Software Engineering Institute (SEI). This model is meant to

- guide the implementation and management of operational resilience activities
- converge key operational risk management activities
- define maturity through capability levels
- enable maturity measurement against the model
- improve an organization's confidence in its response to operational stress and crisis

The CERT-RMM provides the framework from which the CRR is derived—in other words, the CRR method bases its goals and practices on the CERT-RMM process areas.

This guide is intended for organizations seeking help in establishing a vulnerability management process. The process areas described include

- developing a vulnerability analysis and resolution strategy
- developing a vulnerability management plan
- developing a vulnerability discovery capability
- assessing the vulnerability management activities
- managing exposure

More specifically this guide

- educates and informs readers about the vulnerability management process
- promotes a common understanding of the need for a vulnerability management process
- identifies and describes key practices for vulnerability analysis and resolution and vulnerability management
- provides examples and guidance to organizations wishing to implement these practices

The guide is structured as follows:

I. Introduction—Introduces the *CRR Resource Guide* series and describes the content and structure of these documents.

II. Vulnerability Management—Presents an overview of the vulnerability management process and establishes some basic terminology.

III. Define a Vulnerability Analysis and Resolution Strategy—Provides an approach for determining the contents of an appropriate strategy.

IV. Develop a Plan for Vulnerability Management—Outlines a plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization's needs.

V. Implement the Vulnerability Analysis and Resolution Capability—Outlines an approach for putting your plan, team, and tools into operation in support of the organization.

VI. Assess and Improve the Capability—Outlines the process for improving your organization's ability to discover and resolve those vulnerabilities most pertinent to your organization and adjust your plan accordingly.

VII. Conclusion—Provides contacts and references for further information.

Appendices

A. Vulnerability Management Resources

B. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Audience

The principal audience for this guide is individuals responsible for the management, analysis, and disposition of both cyber and physical vulnerabilities affecting an organization's cyber resilience. This includes executives responsible for establishing policies and priorities for vulnerability management, managers and planners responsible for converting executive decisions into plans, and the operations staff that implements the plan and participates in vulnerability disposition.

II. Vulnerability Management

Overview

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment. The CRR resource guides all take a common approach, derived from the CERT-RMM, to describing a domain in terms of a process and its phases. This guide divides the vulnerability management process into four phases, as shown in Figure 1:

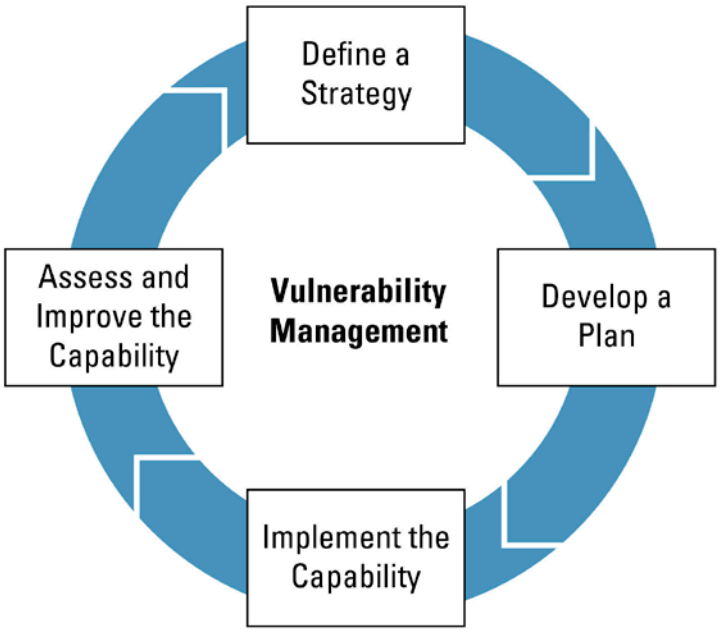

Figure 1: The Vulnerability Management Process

This guide will use an all-encompassing definition of vulnerabilities.

> ***vulnerability:*** *"[P]hysical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard." DHS Risk Lexicon, 2010 Edition*[4]

When discussing vulnerabilities, we are discussing the feature or condition that, if exploited by a threat (natural or man-made), renders an entity (i.e., an entire organization or any of its constituent parts) susceptible to a risk. The CRR focuses on a specific critical service of the organization. Each aspect of the service is discussed in terms of the various assets that support the service. A vulnerability in the service is a result of a vulnerability in one or more of its assets. Assets are divided into the categories of people, information, technology, and facilities.

Vulnerability management is a key component in planning for and determining the appropriate implementation of controls and the management of risk. It is reasonable to say that vulnerability management is central to cyber resilience. The topics of the other CRR domains provide information about vulnerable conditions (Asset Management, Configuration and Change Management, External Dependencies Management, and Situational Awareness) or provide for a response to the vulnerable conditions (Controls Management, Incident Management, Service Continuity Management, Risk Management, and Training and Awareness). Vulnerability management assures that the organization understands its weaknesses so that it can plan accordingly.

Exploitation of a vulnerability by a threat results in a risk to the organization. Expanding the discussion from *what are the vulnerabilities* to *how vulnerable is the organization to disruption* or *what is the impact of exploiting this vulnerability* moves beyond the domain of vulnerability management into a discussion of risk management. It is in risk management that we seek to quantify the impact of a realized hazard. This context is discussed more completely in the *Risk Management Resource Guide*, Volume 7 of this series. An organization's resolution of vulnerabilities and its disposition of risk overlap to a large degree. This resource guide will discuss aspects of risk management as required to clarify the analysis, categorization, and resolution of vulnerabilities.

During the vulnerability management process, the organization may often discover vulnerabilities that lead it to develop requirements and criteria for controls. During the controls management process, the organization develops, implements, and improves the controls that mitigate the effect of a hazard. The *Controls Management Resource Guide*, Volume 2 of this series, discusses controls that mitigate the effect of a hazard.

> *Vulnerability management is primarily a process of understanding the organizational disposition. It is a key component in planning for and determining the appropriate implementation of controls and risk management. See the Controls Management Resource Guide, Volume 2 of this series. Also see the Controls Management (CTRL) process area in the CERT-RMM for more detailed guidance on how to identify controls for assets.*[5]

This guide details each of the steps in the vulnerability management process.

Define a Vulnerability Analysis and Resolution Strategy

The first phase of developing a capability is to define a strategy for achieving the organization's goals. The strategy aligns the vulnerability management process to the organization's requirements and critical success factors. Defining the strategy includes gathering input and support from all stakeholders, an activity that forms the initial engagement strategy.

This guide lays out the discrete steps for developing a strategy that implements the vulnerability management program as described above:

- Determine the scope of vulnerability management.
- Determine approved methods of vulnerability assessment.
- Resource the activities.

Develop a Plan for Vulnerability Management

The strategy needs to be converted into a plan with rules and guidelines for the vulnerability management teams. They need to understand what is expected of them and how they will use the resources they have. The planning phase consists of the following steps:

- Define and document the plan.

- Define measures of effectiveness.
- Define training requirements.
- Determine tools aligned to the strategy.
- Identify sources of vulnerability information.
- Define the roles and responsibilities.
- Engage stakeholders.
- Develop a plan revision process.

Implement the Vulnerability Analysis and Resolution Capability

In this phase of the process, the organization actually implements the vulnerability management plan and conducts vulnerability analysis and resolution activities. It makes use of the methodologies, tools, and sources defined in previous phases and mitigates the organization's exposure to the vulnerability based on the time frames agreed to in the plan. Throughout the performance of vulnerability analysis and resolution, the organization takes steps to ensure that the vulnerability is tracked, improvement information is collected, and the risk management process is engaged where appropriate.

The following are the foundational steps in the implementation of the vulnerability management plan:

- Provide training.
- Conduct vulnerability assessment activities.
- Record discovered vulnerabilities.
- Categorize and prioritize vulnerabilities.
- Manage exposure to discovered vulnerabilities.
- Determine effectiveness of vulnerability dispositions.
- Analyze root causes.

Assess and Improve the Capability

Vulnerability management requires an organization to understand and assess two specific capabilities: the discovery of vulnerabilities and the analysis of pertinent vulnerabilities. The discovery capability requires the expertise to assess the assets and associated processes of the critical services. The organization must also make sure that the discovery capability covers an appropriately comprehensive portion of the organization. Analysis is the ability to determine the extent of the vulnerability and its anticipated effect on the organization and its critical services. Assessing the overall vulnerability management capability ensures that both analysis and discovery are meeting the organization's needs.

The following are the core foundational steps in the assessment and improvement of vulnerability management:

- Determine the state of the program.
- Collect and analyze program information.
- Improve the capability.

Organizations that already have vulnerability management plans can use this resource guide to assess and improve them.

III. Define a Vulnerability Analysis and Resolution Strategy

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin to establish a vulnerability analysis and resolution strategy.

	Input	Guidance
✓	Scoping statement	• Identify the assets and services to be assessed and monitored. • Determine the operational environment comprising the areas of concern. • Define objectives.
✓	Identify stakeholders	The list of stakeholders should be aligned to the scoping statement and include all appropriate internal and external entities. Potential candidates include • executive and senior management • heads of business lines, especially critical services owners • information technology • legal • board of directors • technology vendors • regulators and auditors • compliance personnel
✓	Define regulatory and other legal requirements.	These documents provide requirements for the performance of vulnerability management. They are necessary but rarely sufficient. The documents should be available as references when documenting the strategy. • Obtain pertinent regulatory requirements. • Obtain service-level agreements. • Obtain all other legal obligations.
✓	Stakeholder investment	Stakeholders must acknowledge their intent to adhere to and support the strategy.
✓	Management involvement	• Acknowledgement from management defining budgeting support • Acknowledgement from management defining alignment to internal policy requirements • Aligning vulnerability data collection and distribution activities with identified resilience needs and objectives

Step 1. Determine the scope of vulnerability management.

Vulnerabilities affecting an organization's services and the associated cyber assets are broad and varied. Step 1 is the key defining activity for the vulnerability management process. It outlines the appropriate scope for the organization's capabilities and areas of concern. This is where the organization decides which assets and services need to be assessed and how comprehensive that assessment must be.

Discussions of cyber resilience often suffer from a myopic focus on virtual environments alone. Physical threats affect cyber assets just as cyber assets affect physical services and assets. When assessing the vulnerability of your service, the CRR is concerned with the effect of cyber components on the critical

services. However, the threat to those cyber components may be the result of non-cyber activities or vulnerabilities. Mitigations and resolutions against cyber vulnerabilities may also require non-cyber solutions. These types of vulnerabilities include unsecured server rooms, flooding, work capacity of the personnel, and other vulnerabilities not specific to the cyber operations of the system and related services.

"The identification and remediation of technical vulnerabilities are means for mitigating operational risk, but they do not fully constitute the activities of risk management." CERT-RMM[6]

A. Document the candidate assets and services to be assessed and monitored. In this activity, the organization is primarily focused on documenting all possible candidates for assessment. Resource constraints will impact the assessment and monitoring that the organization will actually be able to accomplish, which will be determined in later steps. Stakeholder should be solicited for their input concerning their critical services and areas of concern.

- Are all stakeholder assets and services represented?
- Define the criticality of stakeholder assets and services.

B. Determine the operational environment for analysis and monitoring. The operational environment defines the types of exposure experienced by assets being monitored. Exposures are descriptions of threats posed by the asset or threats to the organization as a result of a vulnerability in that asset. The environment should be defined by those exposures to the threats of greatest concern.

- Detail both cyber and non-cyber vulnerabilities.
  - Can the asset be affected by physical or cyber threats?
  - Will those threats affect the asset's function or role in cyber resilience?
- Obtain stakeholder input concerning vulnerabilities in the operational environment of their services and assets.
- Obtain third-party threat assessment as needed. The organization may not have the expertise to address all aspects of its operational environment.

Table 1: Asset Types Mapped to Examples of Exposure

Asset Type	Scope Example
People	Employee trust and reliability
Information	Payment information accessibility and distribution
Technology	Database availability
Facilities	Environmental systems availability

Step 2. Determine approved methods of vulnerability assessment.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1: Preparation for vulnerability analysis and resolution activities is conducted.	
2. Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR: SG1.SP2]	**DE.CM**: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
Goal 2: A process for identifying and analyzing vulnerabilities is established and maintained.	
1. Have sources of vulnerability information been identified? [VAR: SG2.SP1]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources

Vulnerability assessments need stakeholder and management support. Certain methods must be thoroughly understood and carefully planned for, both operationally and legally. Penetration testing (physical and virtual) may run afoul of law enforcement or even an organization's own security force. The selected assessment methods should be cleared by the appropriate stakeholders. The methods should be reviewed by legal authority as well as the operational stakeholders.

A. Determine the methods required by regulation. The organization is likely to be bound by industry regulation. Review the requirements of the related regulations such as the Payment Card Industry (PCI) Data Security Standard (DSS) or the Health Insurance Portability and Accountability Act (HIPAA). Some regulations, such as the PCI DSS, require vulnerability assessments by approved vendors. The vulnerability analysis and resolution plan should account for the requirements of the regulation.

B. Determine the methods required to meet the operational requirements. Methods must address the vulnerabilities, services, and assets of concern as determined by the scope of the vulnerability assessment (established in Step 1). The organization should ask the following:

- Do the candidate methods produce information on vulnerabilities within scope?
- Do chosen methods enable the discovery of unanticipated vulnerabilities?

If the methodology focuses on the impact to the service, a detailed decomposition of the assets supporting the service will highlight what each asset provides the service. With this information and input from the stakeholders, the organization increases the likelihood of discovering and better prioritizing events that could impact the service.

C. Determine the legal implications.

- What are the legal requirements to enable the organization to employ the determined methods?
- What are the legal requirements to enable third parties to employ the determined methods?

D. Determine the impact imposed by candidate methods. Certain methods may impose untenable operational impact. Vulnerability discovery methods could cause system down time or negatively impact the job performance of personnel.

- Define methods restricted by legal constraints.
- Define methods restricted by operational constraints.
- Define the choice of methods according to determined restrictions.

E. Choose the methods to be employed. After determining the criteria, the organization should be left with a choice of methods that meet the operational requirement, operational performance constraints, legal responsibility, and impact.

Step 3. Resource the activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.	
1. Has a vulnerability analysis and resolution strategy been developed? [VAR: SG1.SP2]	**PR.IP-12:** A vulnerability management plan is developed and implemented

Resourcing includes staffing. Stakeholders may have roles in the authorization and performance of vulnerability-related functions. Developers may be required to scan their own machines and provide the results

to the vulnerability management team for analysis. Personnel may be responsible for checking that the server room doors are locked when not occupied. Everyone may be responsible for assuring all building occupants are badged appropriately. Some of these activities may require either financial or personnel commitment. Stakeholders, including management, will have to commit to supporting vulnerability management. The organization will determine roles and responsibilities during the development of the plan (see Section IV, Step 6).

A. Determine stakeholder resource responsibility. Stakeholders include the people identified as having a role in authorization and also senior managers and executives of the units where the assets reside. They must understand and agree to the need for remediation and the associated time frames for the corrective actions. These actions may cause disruptions to the normal business operation of their unit. Effects on operations must be understood, and stakeholders must be given the opportunity to address their concerns.

B. Define a budget. When defining a budget, the organization may need to readdress the scope. The budget will ultimately define the capability and greatly impact priorities. Budgetary constraints may limit capabilities.

Output of Section III

	Output	Guidance
✓	Definition of scope	Scope should clearly define the operational restrictions and the organization's capabilities and areas of concern.
✓	Documented vulnerability analysis and resolution strategy	The results of the strategy definition have been clearly documented so that they can inform the development of the process plan.
✓	Framework for vulnerability analysis and resolution plan	The strategy has defined the framework structure for the process plan to be developed. All beginning requirements for the plan should be determined. The organization is now ready to define the roles and responsibilities in the plan.
✓	Representation and investment of stakeholders	The role of and interface to all stakeholders is clearly defined, and all parties have committed.
✓	Representation and investment of management	Management has committed to its role as a stakeholder in this process.
✓	Draft budget	The budget will guide the establishment of both priorities and capabilities.

IV. Develop a Plan for Vulnerability Management

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin planning for vulnerability management.

	Input	Guidance
✓	Vulnerability management strategy	The strategy was developed in Section III and is the basis for the vulnerability management plan.
✓	List of stakeholders	Stakeholders need to understand the need for vulnerability management and agree to the remediation time frames. Potential candidates include • executive and senior management • heads of business lines, especially critical services owners • information technology • legal • board of directors • technology vendors • regulators and auditors • compliance personnel
✓	Management support	Senior management endorses the establishment of a vulnerability management program, assigns budgets, and implements the processes and operation of the plan.
✓	Budget for vulnerability management	The budget drives identification of vulnerabilities. Tradeoffs for developing expertise in-house or using a service should be considered along with long-term costs such as program and skills maintenance.

Step 1. Define and document the plan.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.	
1. Has a vulnerability analysis and resolution strategy been developed? [VAR: SG1.SP2]	**PR.IP-12:** A vulnerability management plan is developed and implemented
2. Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR: SG1.SP2]	**DE.CM**: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
1. Have sources of vulnerability information been identified? [VAR: SG2.SP1]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources
6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented

This step takes the strategy that was developed for vulnerability management and creates a plan for implementing it. The strategy provides the direction, and the plan defines the specifics. For instance, the strategy might indicate that vulnerability scanning will be performed on all assets. The plan will detail how that is to be accomplished because it may be impractical to scan everything at one time. Different asset types will most likely require different tools and techniques to meet the plan objectives. For instance, a network vulnerability scanner may be used for technology, a guard making rounds may be used for facilities, and periodic background checks may be used for people.

A. Build the vulnerability management team. The plan for vulnerability management may need to draw on inputs from different operating units of the organization. For instance, to understand the requirements around patching a particular product, the data security team will need inputs from the server team. Likewise, the physical security team provides inputs on how to secure physical assets.

B. Coordinate with risk management. Vulnerabilities present a risk to the organization. The vulnerability management team should coordinate with the risk management team to determine when their processes should be executed in conjunction with each other.

C. Define standard remediation timelines. A vulnerability classification scale, such as critical–high–medium–low should be defined for how a vulnerability will be classified. Associated with each level of this scale should be a remediation timeframe defining how many days the organization can allow a discovered vulnerability to exist.

D. Define how vulnerabilities should be documented. Ideally, all discovered vulnerabilies should be placed into a central repository. This will facilitate the tracking of remediation efforts and provide information of historical relevance. Additionally, the information may be used as part of measuring effectiveness.

E. Define how exceptions should be handled. Sometimes, a given vulnerability cannot be resolved in a timely manner. The plan should define how to handle these situations, such as by creating a risk using the risk management process, and what level of management must be involved in the decision to exceed the standard remediation timelines.

F. Define periodic activities. Generally, vulnerabilities are introduced only when a change occurs in the environment. This is true of both physical and cyber vulnerabilities. The periodicity of the vulnerability management activities should account for change management and information awareness time frames. Table 2 gives example periodic vulnerability management activities for each asset type.

Table 2: Example Periodic Vulnerability Management Activities for Asset Types

Asset Type	Example Periodic Activities
People	Clean desk checks, reinvestigations, information awareness activities
Information	Monitoring sources (e.g., email, Twitter) for relevant information
Technology	Scanning, change management
Facilities	Security checks by roving guards

G. Define proactive activities. Watching mailing lists, Twitter, blogs, and similar information assets is a reactive activity. Scanning and penetration testing, on the other hand, are proactive activities and need to be scheduled. The plan should detail how often these activities are performed and on what portions of the environment. When scanning, the organization should consider the following:

- with or without firewall rules

- internal or internet source of scanning
- level of scanning
- in-house or third-party scanning

Organizations can also conduct proactive activities to discover vulnerabilities in nontechnology assets, as in the following examples:

- facilities
  - Is the server room door locked at the end of the day?
  - Do entry and exit logs balance?
  - Are the fire suppression systems serviced as required?
- people
  - Has there been a change in their work behavior?
  - Has there been a change in their personal life (e.g., finances)?

Step 2. Define measures of effectiveness.

To understand how well the organization is performing vulnerability management activities, the organization must measure their effectiveness. The planning team should determine how to measure effectiveness, any reporting requirements, and the necessary processes and tools.

Step 3. Define training requirements.

Meeting the requirements of vulnerability management may require two types of training: end user training and practitioner training. The *Training and Awareness Resource Guide*, Volume 9 of this series, details how the organization should identify, conduct, and evaluate this training.

A. Identify end user training. Within its vulnerability management strategy, the organization may have determined that its general employee population should receive specific training to reduce the likelihood of becoming the source of an incident. Training related to vulnerability management can address, among other things,

- phishing attacks
- safe surfing

B. Train practitioners. This training focuses on educating the personnel responsible for vulnerability management on the organization's methods and tools. This could include

- how to use the approved tools
- procedures for vulnerability management, including how they are tracked, time frames for remediation, and others
- roles and responsibilities
- certifications

Practitioners may be spread out in different areas of the organization. For instance, managers and human resources personnel may be responsible for monitoring vulnerability information for people assets, while site security may be responsible for the facilities.

Step 4. Determine tools aligned to the strategy.

In this step, the organization identifies which tools it should use to execute the methods indicated by the strategy. Some methodologies may require more than one tool to conduct a comprehensive assessment.

A. Identify candidate tools. Research what tools or services can be used to meet the needs of each methodology.

B. Test tools. Evaluate each of the candidate tools or services to determine if they are appropriate for the environment. A key fact to determine is whether the tool fulfills all needs or another tool is needed to fill the gaps.

C. Publish authorized tool list. The finalized list of tools should be published so that anyone within the organization can ascertain what tools they are allowed to use.

D. Define the exception process. Changing situations may necessitate the use of a new tool to meet a critical need such as validating a new vulnerability or assisting in incident response. The organization should define a process to authorize the use of a new tool for a period of time.

E. Conduct periodic reviews. Review the tools periodically to determine if they are still meeting the needs of the organization. Likewise, review new tools and services, which may provide a better solution than an existing tool.

Step 5. Identify sources of vulnerability information.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
1. Have sources of vulnerability information been identified? [VAR: SG2.SP1]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources

Good sources of vulnerability information are essential to safeguarding the organization. There are many sources of this information (see Table 3 in Part B below) and one source will in all likelihood not be sufficient especially due to the varying asset types. The organization will need to evaluation which ones will best fit their needs and resources.

A. Identify assets in use. To understand what vulnerability information an organization needs, it must know what assets are in use. This information may be obtained from asset inventories for the respective asset type. When talking about vulnerabilities, most people in the cyber field immediately think of the hardware and software components of their IT infrastructure. However, other assets are also vulnerable, namely people and the facilities housing the technology, information, and people.

See the Asset Management Guide, Volume 1 of this series, for help with asset management practices.

For technology assets, the following information will be needed:

- model numbers for hardware
- version numbers for software
- location of the component

Ideally the organization will store this information in an asset database, which the organization will need when making the corrective actions pertinent to a particular vulnerability.

When identifying technology assets, do not just focus on the workstation and servers in the environment. Also include the IT infrastructure components, such as firewalls, routers, switches, and load balancers, that are in use.

B. Identify sources of vulnerability information. With the list of unique assets to be monitored in hand, the organization must identify the sources of vulnerability information for each asset. Table 3 identifies some potential sources, and an internet search for vulnerability information about a particular item may reveal others.

Table 3: Sources of Vulnerability Information

Source	Information
Vendors	Vendors, and technology vendors in particular, often provide advisories along with patches for security vulnerabilities.
Mailing lists	Lists such as Bugtraq and Full Disclosure provide vulnerability information about a wide range of products, though, as a result, the email volume is quite heavy.
Department of Homeland Security (DHS)	US-CERT and ICS-CERT provide security advisories for IT assets. DHS also provides onsite facility inspections through their regional PSA (Protective Security Advisor) program.
Information Sharing and Analysis Centers (ISACs)	There are various ISACs that focus on particular sectors and provide their members various services such as advisories and threat warnings tailored per sector.
User groups	User groups for a particular product can also provide information about threats and vulnerabilities in that product. User groups typically communicate through a mailing list and may not always contain security-relevant information. However, it is likely that someone may be monitoring the list for support reasons, see a security advisory, and bring it to the vulnerability management's team attention.
InfraGard	The Federal Bureau of Investigation (FBI) runs the InfraGard program, which provides its vetted members information about current threats and includes information such as source information and methodologies being used.
Twitter	Monitoring Twitter can provide information about activities that may affect a particular location or the organization as a whole.
Security services	Managed Security Service (MSS) vendors provide vulnerability-related services such as tailored advisories and vulnerability scanning for a fee.

While external sources can provide information on vulnerabilities inherent in a particular asset, they cannot reveal vulnerabilities that are caused by misconfiguration of a technology asset or a failure in training of people assets. The organization may decide to use tools to identify these weaknesses. For instance, a vulnerability scanner or a penetration test may be run periodically against technology assets. Likewise, to assess training issues, the organization can periodically send fake phishing emails to employees to see who clicks on them.

Some sources of vulnerability information may be internal to the organization. Managers and human resources staff may observe abnormal behavior in other employees that could indicate malicious actions. Periodic background checks of employees may be another source of information.

For facility assets, the organization should consider other sources of information, such as weather forecasts, on events that could impact the on-site operations.

Step 6. Define the roles and responsibilities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented

By this step, the organization has nearly completed the development of a plan for vulnerability management: sources of information have been identified and the set of tools to be used has been defined. The organization should now determine who should be executing the plan and what their responsibilities are. The planning team will identify units or individuals of the organization who will be charged with performing the vulnerability management functions and assign them into the following roles.

A. Monitoring roles. These personnel are responsible for monitoring the various sources of vulnerability information and taking the appropriate action. Monitoring roles should be assigned to those who
- analyze the relevance of vulnerabilities to the organization
- log the vulnerability information into the vulnerability repository
- alert the remediation team

B. Remediation roles. Personnel from different parts of the organization may have responsibilities such as
- analyze the impact of patches on the organization
- develop in-house workarounds to the vulnerability if none are available
- gain authorization to make the changes, possibly through change management (see the Configuration and Change Management Resource Guide, Volume 3 of this series)
- invoke the risk management process if the vulnerability needs to remain open past defined thresholds

C. Authorization roles. Personnel in this role are responsible for understanding their environments and must review the corrective actions to determine if there may be any adverse effects. They are part of the change management process and act accordingly. An emergency change request process should be in place to handle corrective actions that must be addressed immediately.

Step 7. Engage stakeholders.

Stakeholders include those with authorization roles, as identified in Step 6, as well as senior managers and executives of the units where the assets reside. Because vulnerability management may not be constrained just to IT functions, the organization may need to identify stakeholders in the physical security and human resource departments in addition to others, depending on the needs of the plan.

Stakeholder responsibilities include
- providing input about their unit's particular requirements
- championing the vulnerability management plan to their respective teams
- agreeing to remediation time frames

Step 8. Develop a plan revision process.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
2. Is the information from these sources kept current? [VAR: SG2.SP1]	**DE.DP-5:** Detection processes are continuously improved **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources **PR.IP-7**: Protection processes are continuously improved

Any good plan needs to change as the environment around it changes. Organizations should review their vulnerability management plan at least annually to determine if it is meeting the organization's needs.

A. Determine if changes have occurred. To determine if the plan needs to be updated, review what has happened to the organization since the last plan review. Some questions to consider:

- Has new technology been introduced to the organization?
- Have new facilities been added or removed from the organization?
- Has the organization acquired any other organizations?
- Have any components of the organization been divested from the organization?
- Have new methodologies been introduced to detect vulnerabilities?
- Have new people been added, removed, or outsourced?

A *yes* answer to any of these questions indicates that a more in-depth review of the plan is warranted.

B. Review the changes. Determine the impact of the change to the organization, and make the appropriate changes to the plan.

C. Update toolset if necessary. The change in the plan may require an update in the tools used to detect vulnerabilities.

D. Update sources of vulnerability information. If a change has introduced something new (facilities, technology, etc.) to the organization, it is imperative that the organization identify a source of vulnerability information for the new asset. Most likely, a relationship with the new asset's vendor would have been recently established, and the vendor would be the primary source of information. However, the organization may want to consider other sources such as user groups. Additionally, if any of the current sources of information tailor what they send based on a profile, it should also be updated.

Output of Section IV

	Output	Guidance
✓	Vulnerability management plan	Engage stakeholders and ensure they all agree on the time frames for discovery and remediation. Ensure roles and responsibilities are assigned and defined.
✓	Vulnerability management process	Different assets will have different process documents. Ensure consistency and integration across all process documents.
✓	List of approved tools	Make the list available to everyone and define the process for the use of new tools.
✓	List of sources of vulnerability information	Understanding what is at risk in the environment is paramount so the organization can determine appropriate sources of vulnerability information.
✓	Vulnerability management revision process	Change happens, and the organization needs a process to update the various components of the plan.

V. Implement the Vulnerability Analysis and Resolution Capability

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin implementing the vulnerability analysis and resolution capability.

	Input	Guidance
✓	Vulnerability management plan	Engage stakeholders and ensure they all agree on the time frames for discovery and remediation. Ensure roles and responsibilities are acknowledged.
✓	Vulnerability management process	Different assets will have different process documents. Ensure consistency and integration across all process documents.
✓	List of sources of vulnerability information	The source information tells the vulnerability management team what they should be monitoring to start the process.
✓	Definition of roles and responsibilities	Everyone should understand what is expected of them in relation to the handling of vulnerabilities.
✓	Approved tools list	The team uses the tested and approved tools on this list to discover, track, and determine the disposition of vulnerabilities in the environment.

Step 1. Provide training.

The organization must ensure the personnel executing the process are fully trained on the process itself as well as the planned tasks. Personnel should possess the skills to appropriately execute the tasks defined. Individuals need to be trained to use the specific tools, techniques, and methodologies. They must understand their role, the roles of the stakeholders, any third-party assets, and the workflow. Training must emphasize key decision points and operational restrictions.

See the Training and Awareness Guide, Volume 9 of this series.

A. Train personnel on the process. All personnel involved in vulnerability management should understand the processes associated with their duties. Understanding of the inter-relationships with other processes such as change management must be emphasized to ensure a coherent approach.

B. Train personnel on the tasks. In addition to the process, personnel need to understand what their tasks are and how to perform them according to the plan that has been developed.

Step 2. Conduct vulnerability assessment activities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
3. Are vulnerabilities being actively discovered? [VAR: SG2.SP2]	**DE.CM-8:** Vulnerability scans are performed **ID.RA-1:** Asset vulnerabilities are identified and documented

This step entails conducting vulnerability assessment activities to discover any existing vulnerabilities in the organization. As previously discussed, the assessment methods should address all types of assets supporting the critical service, including information, technology, people, and facilities. Physical security audits, environmental control checks (HVAC, fire suppression), organizational threat assessments, and cyber vulnerability scanners are all key components of a thorough organizational vulnerability assessment.

A. Execute vulnerability scans. Scanning can be done in house or may be contracted out to a third party. Determine the capabilities of the organization's personnel and supplement with external assistance as needed. Technically capable in-house teams may not always be available; they could be busy with remediation or working with the stakeholders.

B. Execute vulnerability assessments. Vulnerability assessments, also known as penetration tests, test to a greater depth than a scanner. These are more comprehensive than audits or scans and generally include physical vulnerabilities to the systems. Because of they are more comprehensive and can not be automated, vulnerability assessments are not typically performed across all assets the organization uses and must be tailored for a specific instance.

Penetration tests (or pen tests) are antagonistic in that third-party testers usually compete against the organization's personnel to gain access to assets that they normally would not have. The organization should discuss the penetration test with stakeholders ahead of time, and everyone involved should understand that it is a safe event with the goal of learning. Focusing on beating the penetration testers or gaming the test itself will not benefit the organization (though it may boost the morale of the intrusion response team). Rather, the vulnerability management team should see the penetration test as an opportunity to learn about their daily operations strengths and weaknesses.

Step 3. Record discovered vulnerabilities.

Vulnerabilities must be recorded in a vulnerability repository. This enables organizations to approach vulnerability management in a structured and trackable way. Discovered vulnerabilities are not only useful for hardening the organization's current posture but also for planning organizational changes to operations. Historical data, including data on vulnerabilities, can be a deciding factor in the implementation of an architecture change.

A. Log the vulnerability into the repository. To ensure that the vulnerability is tracked to closure, it should be logged into a repository. Some fields that the organization may want to record in the repository are

- discovery date and time
- affected assets
- priority
- categorization

- source
- owner
- analysis notes
- current status
- closure date and time

B. Assure access control of the repository. Remember that this information is highly sensitive: it is basically a road map of the organization's exposures. Treat this information appropriately. Limit access to the repository to those who have a need to know this information: primarily the vulnerability management team and its management but possibly personnel from the risk management team as well.

Step 4. Categorize and prioritize vulnerabilities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
4. Are vulnerabilities categorized and prioritized? [VAR: SG2.SP3]	**PR.IP-12:** A vulnerability management plan is developed and implemented
5. Are vulnerabilities analyzed to determine relevance to the organization? [VAR: SG2.SP3]	**PR.IP-12:** A vulnerability management plan is developed and implemented
Goal 3 - Exposure to identified vulnerabilities is managed.	
1. Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1]	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks
3. Is the status of unresolved vulnerabilities monitored? [VAR: SG3.SP1]	**PR.IP-12:** A vulnerability management plan is developed and implemented

In this step, the organization determines its relationship to the findings of vulnerability discovery. Do the findings affect the critical services? What is the impact? Are there any relationships among the findings? This is the first step in the analysis of the vulnerabilities.

Analysis should focus on the characterization of the vulnerabilities and how to remediate them.

A. Analyze for relevance. Is the vulnerability pertinent to the organization's operations? Information channels, penetration testing teams (internal and third party), and vulnerability discovery tools will produce a wealth of information. Those findings that affect only the assets the organization does not employ can be ignored, but they should be maintained for reference when planning changes to the organization. If a technology has a high vulnerability rate, the organization may decide to choose a different technology to avoid the remediation workload and associated costs.

B. Determine responsibility. The vulnerability management team may discover the vulnerabilities but is generally not responsible for their mitigation or resolution. The vulnerability team will need to inform the appropriate stakeholders. Appropriate disposition of the vulnerabilities requires coordination with the stakeholders for prioritization and planning.

C. Prioritize. When prioritizing vulnerabilities, the vulnerability team must coordinate with the risk management team. In some organizations, the vulnerability and risk management teams may be composed of the same personnel. When these teams are combined, the tracking, categorization, and prioritization of vulnerabilities are usually merged into the equivalent risk processes.

The severity of a vulnerability is often used for prioritization in that highs are typically patched quicker than lows. Some sources of vulnerability information (see Table 4 for some examples) may assign severities while others will not. Regardless, the organization should ask itself what a severity rating may indicate and what it means to the organization. For instance, a high-severity vulnerability on two internal assets may not be as critical as a vulnerability affecting all external-facing assets. The severity the information source has selected may not match how the organization views the vulnerability, and the organization will need to adjust the severity rating. Depending on the nature of the vulnerability, it may not have the same severity rating throughout the organization. Using the methodology identified in the vulnerability management strategy, the organization should evaluate the vulnerability's priority in relation to the organization's architecture and operations.

Table 4: Example Sources of Prioritization and Severity Guidance

Source	Reference
CVSS	http://nvd.nist.gov/cvss.cfm
DISA Security Technical Implementation Guides	http://iase.disa.mil/stigs/
Vendors	
Adobe	http://helpx.adobe.com/security/severity-ratings.html
Microsoft	http://technet.microsoft.com/en-us/security/gg309177.aspx
Redhat	https://access.redhat.com/site/security/updates/classification/

Step 5. Manage exposure to discovered vulnerabilities.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
5. Are vulnerabilities analyzed to determine relevance to the organization? [VAR: SG2.SP3]	**PR.IP-12:** A vulnerability management plan is developed and implemented
6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented
Goal 3 - Exposure to identified vulnerabilities is managed.	
1. Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1]	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks

Now that the organization has determined that the vulnerability is relevant and assigned it a priority rating, it takes action to reduce its exposure. Common risk dispositions are to accept, avoid, mitigate, or transfer operational risk.

A. Determine disposition methodology. The disposition action varies based on the nature of the asset and the source of the vulnerability information.

- *Acquire vendor-provided solution.* When vendors are made aware of a vulnerability in their product, they will make changes to eliminate the vulnerability. For information technology systems, these changes are called patches.
- *Change configuration.* In some cases, the corrective actions might be to change the configuration of the asset to eliminate the vulnerability. If a network security scan reveals an unused service, the

solution might be to turn the service off. For a physical access vulnerability, changing how someone reaches the asset might be the solution.

- *Apply workaround.* If there is no patch or configuration options that would remove the vulnerability, another method to reduce the risk is to place controls in the environment that can prevent the vulnerability from being exploited.
- *Accept the risk.* If there is no practical or cost effective method of mitigating at least part of the risk of the vulnerability, the risk management process should be invoked to define the risk and gain acceptance for leaving it open.

B. Test disposition. The organization should test the selected disposition prior to general deployment to determine its impact on the operational environment. This is especially true for technology solutions, but it also applies to any change. For instance, erecting an entry control gate for the parking lot may inadvertently cause cars to be backed up into the roadway. In many cases, the change management process will mandate this step.

C. Deploy disposition method. The tested disposition method should now be deployed into the environment using the targeted time frames for the priority of the vulnerability. Use of the change management system is encouraged to allow for the scheduling and approvals needed to make the change. In some cases, the teams performing the disposition may be different from the team managing the vulnerability. For instance, patching Windows vulnerabilities might be performed by the server and workstation teams, but managing the vulnerability might be performed by the information security team.

D. Track to resolution. All corrective actions should be tracked in the vulnerability management repository until the selected disposition methodology has been applied for the vulnerability throughout the organization's environment. If a disposition deployment is delayed and is going to miss the vulnerability's targeted time frame for resolution, the exception process developed in conjunction with the plan should be invoked. The organizations should note any abnormal effects caused by the disposition, along with their resolution, in the repository. If the organization uses a change management tool, each of its entries should refer to the corresponding entry in the vulnerability repository, and vice versa. This will facilitate the next step.

If the disposition activity is just a workaround, the organization should continue to monitor for the availability of a vendor-provided solution. When one is available, this "Manage exposure to discovered vulnerabilities" step should be repeated in its entirety.

Step 6. Determine effectiveness of vulnerability dispositions.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented
Goal 3 - Exposure to identified vulnerabilities is managed.	
2. Is the effectiveness of vulnerability mitigation reviewed? [VAR: SG3.SP1]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-7:** Protection processes are continuously improved **RS.IM:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Once the organization has determined the disposition of the vulnerability, it should determine if the disposition is meeting its goals. It is important to understand whether or not the risk of the vulnerability has been either lessened or removed. Depending on how the vulnerability was discovered, the organization may be able to repeat the discovery method to validate the disposition of the vulnerability. For example, if a network scanner or penetration test discovered the vulnerability, rerunning the relevant portion of the test would indicate how the remediation efforts have paid off.

A. Evaluate disposition efforts. The organization should perform tests to confirm that the dispositions have been applied correctly. These tests should assess whether the remediation efforts experienced or caused any problems as well as determine whether the actions addressed the identified vulnerabilities. Depending on the number of components, it may be necessary to spot check that the disposition was completed if there are no automated methods of doing this. If this is the case, management should agree on the sample percentage of systems that represent the population of interest, which should be documented in the plan.

A possible source of information may be the asset inventory if there are automated tools or methods that keep it current.

B. Update vulnerability repository. The vulnerability team should update the repository with the findings of the evaluation.

C. Repeat disposition process as necessary. If the findings of the effectiveness testing indicate that the dispositions are not reducing the risk, the process should be restarted at Step 5, “Manage exposure to discovered vulnerabilities,” to determine a more effective disposition strategy.

Step 7. Analyze root causes.

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	
5. Are vulnerabilities analyzed to determine relevance to the organization? [VAR: SG2.SP3]	**PR.IP-12:** A vulnerability management plan is developed and implemented
6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented
Goal 3 - Exposure to identified vulnerabilities is managed.	
1. Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1]	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks
Goal 4 – The root causes of vulnerabilities are addressed.	
1. Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR: SG4.SP1]	**PR.IP-12:** A vulnerability management plan is developed and implemented **RS.IM:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Root cause analysis (RCA) is a mechanism for gaining a deeper understanding of why an event has happened. From this understanding, a means for correcting and potentially preventing this action from happening again may be developed. For vulnerability management, doing RCA on vulnerabilities enables the organization to prevent repeat vulnerabilities.

> *Some vulnerabilities are outside the control of the organization, which may not benefit from an RCA. Though every vulnerability that is discovered should be considered for RCA, corollary information such as alternative vendors for an asset may be a considered for corrective action.*

The primary reason for performing RCA is to prevent repeat occurrences of the vulnerability. RCAs have a cost, but conducting an RCA on the first occurrence of a vulnerability can prevent future occurrences that could incur greater costs and potentially lead to an incident if exploited.

A. Perform root cause analysis. The organization should analyze the vulnerability to determine why it existed. Some possible causes are

- vendor issue
- misconfiguration
- failure to follow policy or procedures
- poor software design
- improper training
- operational complexity

B. Develop corrective actions to address root cause. Depending on the cause, the organization should develop a corrective action to reduce the chance that the particular vulnerability will occur in the future. Application software developed in-house may need to be tested for vulnerabilities before it is promoted to production, or staff may need to be trained in secure coding techniques. An RCA of a facility vulnerability may suggest architectural changes to prevent other sites from having the same issue.

C. Update the vulnerability repository. As with all actions regarding vulnerabilities, the organization should update the vulnerability's record in the repository with the cause and the corrective actions taken. This will assist with the next phase.

D. Monitor effect of corrective actions. After the organization has taken corrective actions, it should monitor for additional instances of the vulnerability by querying the repository or rerunning detection activities such as scans. Additional instances of the vulnerability may indicate that a root cause has not been addressed, which may require additional corrective actions.

Output of Section V

	Output	Guidance
✓	Vulnerability prioritization guidelines	Vulnerabilities need to be prioritized based on the environment they are found in.
✓	Vulnerability analysis	As each vulnerability is discovered, it is analyzed to determine if it is relevant to the organization. If so, it is categorized, prioritized, logged and a mitigation strategy is developed.
✓	Repository of prioritized vulnerabilities and disposition	A repository is highly recommended for tracking vulnerabilities and maintaining a historical record of actions taken. It can then be queried when new vulnerabilities are discovered to understand what was done before.
✓	Analysis of sources of vulnerabilities	Using root cause analysis to understand why a vulnerability happened gives the organization an opportunity to make changes that can prevent a similar vulnerability in the future.
✓	Analysis of vulnerability disposition capabilities	Monitoring the disposition of vulnerabilities not only gives the organization confidence that vulnerabilities are being correctly addressed, but it also presents opportunities to learn how to improve the process.

VI. Assess and Improve the Capability

Before You Begin

The following checklist summarizes the tasks you will need to complete and the information you will need to gather before you can begin assessing and improving the capability.

	Input	Guidance
✓	Vulnerability management strategy	• Collect the guidance and requirements defined in the strategy.
✓	List of identified stakeholders	• Determine the consumers of vulnerability information. • Determine those who might be impacted by discovered vulnerabilities.
✓	Established measures of improvement	• Measure program outcomes versus stated objectives. • Determine what is actionable knowledge. • Determine required derivative metrics.
✓	Established monitoring program	• Establish a means of collecting the established measures at appropriate intervals.

Step 1. Determine the state of the program.

Before making improvements to the vulnerability management program, the organization must establish the program's current state of performance. The CRR questions themselves, included in Appendix B of this document, are a good point of reference. If the organization has trouble answering the CRR questions, that is a good indicator that the organization needs more information about the state of the program.

A. Review the strategy with stakeholders.

- Are all relevant stakeholders represented?

B. Determine what each stakeholder needs.

- Is the process impacting the appropriate work products?
- What information directly impacts stakeholder processes?
- How are stakeholders using the information?

C. Determine what the current process provides.

- Is the process providing the appropriate work products?
- Is the organization able to answer all of the CRR questions?
- What information is missing?

Step 2. Collect and analyze program information.

The previous step assessed the state of the program to ensure it is performing as intended; this step assesses the outputs of the program to determine whether it is actually achieving the goal of reducing vulnerabilities across the organization.

A. Collect all pertinent work products, policies, and guidance.

- Gather process outputs.
- Gather process policy.
- Gather process plan.
- Gather process strategy.
- Gather standards and guidelines.
- Gather list of stakeholders and external dependencies.
- Compile all reports on measures of effectiveness.
- Gather review activity schedule. This is the schedule determining the periodicity of reviews of the process itself.
- Gather example reports to stakeholders, including reports to management.
- Gather organizational standards for vulnerability management.

B. Analyze the measures of effectiveness.

- Do the measures of effectiveness address the required aspects of the process?
- Are the measures of effectiveness aligned to the critical service?
- Do the measures of effectiveness give actionable information about the work products?

C. Analyze the collected products versus the measures of effectiveness.

- Do work products provide information that is actionable by the stakeholders?
- Are stakeholders adhering to the process?
- Are sources of vulnerability information still current?

D. Determine the risk of not meeting the measures of effectiveness. Here the vulnerability management team must work with the risk analysis team to understand the parameters around risk measurement. Determine best- and worst-case examples from possible responses to the evaluated vulnerabilities. If the difference between the responses to the best and worst cases is small, the effort to meet the measures of effectiveness may not be worth the expenditure. In such a case, the organization should re-address the measures of effectiveness. Measures of effectiveness should be defined by operational requirements and impact.

Step 3. Improve the capability.

Improvement is the act of rectifying the deficiencies found during the analysis of the process. An appropriately defined process achieves the desired goals efficiently and effectively. The organization will have defined its desired effectiveness during the planning process. The analysis performed in Step 2 develops a baseline for understanding the effectiveness of the process. Once the organization understands how well its capability is meeting the measures of effectiveness, the organization addresses how well the measures meet their needs.

A. Address deficiencies in the process as defined by the measures of effectiveness.

- If a metric of one of the measurements is negative, what does that imply about the process?

- Does the deficiency impact the process's ability to mitigate vulnerabilities? discover vulnerabilities? engage stakeholders?
- How does one mitigate that deficiency? What about the process must be changed to address the deficiency?

Improving the capability is iterative. A capability as a whole develops when the organization assesses and improves the process at each developmental stage. How much the organization invests in this part of the process depends on how much information it needs to improve. For young processes, the organization can more quickly and easily collect cruder information and provide quicker and more recognizable changes. In a more mature process, the changes are subtle and require a more mature improvement process to make the appropriate measurements and relate them to the more subtle improvements.

Output of Section VI

	Output	Guidance
✓	Assessment report	• Details the topics presented below
✓	Gaps in asset coverage	• List of assets not covered by the current vulnerability management plan
✓	Gaps in service coverage	• List of services not covered by the current vulnerability management plan
✓	Risks from undiscovered vulnerabilities	• Anticipated effects from the gaps in asset or service coverage
✓	Risks from inaccurate analysis	• Effects from analysis resulting from poor understanding of the service, poor understanding of the roles of the assets, or systemic relations
✓	Report on effectiveness of controls	• Discusses the effect of controls (current and proposed) on discovered vulnerabilities
✓	Proposed process changes	• Discusses findings and their relation to operations; documents suggestions for realignment, capability changes, and capacity adjustments

VII. Conclusion

Establishing and supporting an ongoing vulnerability management program enables an organization to evaluate the effectiveness of its vulnerability discovery, analysis, and resolution capability and provides information guiding the other management domains. The vulnerability management program helps to ensure that the organization maintains a comprehensive understanding of its critical services, meets its responsibility to its stakeholders, and contributes to national critical infrastructure.

The following documents provide broad program guidance:

- *NIST Special Publication SP 800-53* (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) provides a catalog of controls for information systems.
- *NIST Special Publication SP 800-53A* (http:// http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf) provides guidelines for conducting assessments on information systems.
- The *CERT-RMM* [Caralli 2010] is the basis for the CRR and contains more in-depth guidance for establishing practices.

For more information about the Cyber Resilience Review, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov or visit http://www.us-cert.gov/ccubedvp/self-service-crr.

Appendix A. Vulnerability Management Resources

Federal Financial Institutions Examination Council (FFIEC)
http://www.ffiec.gov/

- Information Security Booklet
  http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx

Gartner (requires subscription)
http://www.gartner.com/technology/home.jsp

- *Vulnerability Assessment Technology and Vulnerability Management Practices*
  https://www.gartner.com/doc/2664022?pcp=itg
  - MarketScope for Vulnerability Assessment
    https://www.gartner.com/doc/2586218?pcp=itg
  - Improve IT Security With Vulnerability Management
    https://www.gartner.com/doc/480703

Forrester
http://www.forrester.com/home/

- Vulnerability management articles, tools, and templates (some require a fee)
  http://www.forrester.com/search?tmtxt=vulnerability%20management&searchOption=10001&source=typed

FS-ISAC

- Cyber Intelligence Repository
  https://www.fsisac.com/CyberIntelligenceRepository

HIPAA.com
http://www.hippa.com/

- Security Management Process: Risk Analysis-What to Do and How to Do It [Risk and vulnerability management]
  http://www.hipaa.com/2009/02/security-management-process-risk-analysis%E2%80%94what-to-do-and-how-to-do-it/

International Organization for Standardization (ISO)
http://www.iso.org/iso/home.html

- ISO/IEC TR 20004:2012 Information technology -- Security techniques -- Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 (fee)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50951
  - ISO/IEC 30111:2013 Information technology -- Security techniques -- Vulnerability handling processes (fee)
    http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231

- ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure (fee)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  - National Vulnerability Database
    http://www.nist.gov/itl/csd/stvm/nvd.cfm
    http://nvd.nist.gov/home.cfm
  - NIST IR 7946 DRAFT CVSS Implementation Guidance
    http://csrc.nist.gov/publications/drafts/nistir-7946/draft_nistir_7946.pdf
  - NIST NIST IR 7669 DRAFT Open Vulnerability Assessment Language (OVAL) Validation Program Derived Test Requirements
    http://csrc.nist.gov/publications/drafts/nistir-7669/draft-nistir-7669.pdf
  - NIST IR 7328 DRAFT Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems
    http://csrc.nist.gov/publications/drafts/nistir-7328/NISTIR_7328-ipdraft.pdf
  - SP 800-40 v.2.0 Creating a Patch and Vulnerability Management Program
    http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
  - NIST Publication list
    http://csrc.nist.gov/publications/PubsFL.html

Payment Card Industry (PCI) Security Standards Council
https://www.pcisecuritystandards.org/index.php

- *Payment Card Industry (PCI) Data Security Standard, Navigating PCI DSS – Understanding the Intent of the Requirements v.2.0* See sections 5 and 6, *Maintain a Vulnerability Management Program*
  https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf
- *Payment Card Industry (PCI) Data Security Standard – Security Scanning Procedures*
  https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf
- *PCI Quick Reference Guide*
  https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf
- PCI approved scanning vendors
  https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

SearchHealthIT
http://searchhealthit.techtarget.com/

- *Best of vulnerability management 2013*
  http://searchsecurity.techtarget.com/feature/Best-of-vulnerability-management-2013
  - Access “Vulnerability management programs: A handbook for security pros”
    http://searchsecurity.techtarget.com/ehandbook/Vulnerability-management-programs-A-handbook-for-security-pros

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

- CERT Resilience Management Model
  http://www.cert.org/resilience/products-services/cert-rmm/index.cfm
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  http://www.cert.org/resilience/products-services/octave/index.cfm
  - Vulnerability analysis topics at CERT
    http://www.cert.org/blogs/blog_categories.cfm?getCat=Vulnerability%20Analysis
  - Vulnerability discovery topics at CERT
    http://www.cert.org/blogs/blog_categories.cfm?getCat=Vulnerability%20Discovery

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov

- *Getting Started for State, Local, Tribal, and Territorial (SLTT) Governments*
  http://www.us-cert.gov/ccubedvp/getting-started-sltt
- *Exploit and Vulnerability Databases*
  https://buildsecurityin.us-cert.gov/swa/resources/exploit-and-vulnerability-databases
- Analytical Tools and Programs
  http://www.us-cert.gov/government-users/tools-and-programs
  National Cyber Awareness System
  https://www.us-cert.gov/ncas

Appendix B. CRR/CERT-RMM Practice/NIST CSF Subcategory Reference

Table 5 cross-references CRR Vulnerability Management Domain goals and practice questions to the NIST CSF Categories/Subcategories and the sections of this guide that address those questions. Users of this guide may wish to review the CRR Question Set with Guidance available at https://www.us-cert.gov/ccubedvp for more information on interpreting practice questions. The NIST CSF, available at https://www.us-cert.gov/ccubedvp also provides informative references for interpreting Category and Subcategory statements.

Table 5: Cross-Reference of CRR Goals/Practices and NIST CSF Category/Subcategory Against the Vulnerability Management Resource Guide

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Vulnerability Management Resource Guide Reference
Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.	—	—
1. Has a vulnerability analysis and resolution strategy been developed? [VAR: SG1.SP2]	**PR.IP-12:** A vulnerability management plan is developed and implemented	Section III, Step 3 Section IV, Step 1
2. Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR: SG1.SP2]	**DE.CM**: The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	Section III, Step 2 Section IV, Step 1
Goal 2 – A process for identifying and analyzing vulnerabilities is established and maintained.	—	—
1. Have sources of vulnerability information been identified? [VAR: SG2.SP1]	**ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources	Section III, Step 2 Section IV, Step 1 Section IV, Step 5
2. Is the information from these sources kept current? [VAR: SG2.SP1]	**DE.DP-5:** Detection processes are continuously improved **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources **PR.IP-7**: Protection processes are continuously improved	Section IV, Step 8
3. Are vulnerabilities being actively discovered? [VAR: SG2.SP2]	**DE.CM-8:** Vulnerability scans are performed **ID.RA-1:** Asset vulnerabilities are identified and documented	
4. Are vulnerabilities categorized and prioritized? [VAR: SG2.SP3]	**PR.IP-12:** A vulnerability management plan is developed and implemented	Section V, Step 4
5. Are vulnerabilities analyzed to determine relevance to the organization? [VAR: SG2.SP3]	**PR.IP-12:** A vulnerability management plan is developed and implemented	Section V, Step 4 Section V, Step 5 Section V, Step 7
6. Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	**ID.RA-1:** Asset vulnerabilities are identified and documented **PR.IP-12:** A vulnerability management plan is developed and implemented	Section IV, Step 1 Section IV, Step 6 Section V, Step 5 Section V, Step 6 Section V, Step 7
Goal 3 - Exposure to identified vulnerabilities is managed.	—	—
1. Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1]	**RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks	Section V, Step 4 Section V, Step 5 Section V, Step 7
2. Is the effectiveness of vulnerability mitigation reviewed? [VAR: SG3.SP1]	**DE.DP-5:** Detection processes are continuously improved **PR.IP-7:** Protection processes are continuously improved	Section V, Step 6

CRR Goal and Practice [CERT-RMM Reference]	NIST CSF Category/ Subcategory	Vulnerability Management Resource Guide Reference
	RS.IM: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
3. Is the status of unresolved vulnerabilities monitored? [VAR: SG3.SP1]	**PR.IP-12:** A vulnerability management plan is developed and implemented	Section V, Step 4
Goal 4 – The root causes of vulnerabilities are addressed.	—	—
1. Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR: SG4.SP1]	**PR.IP-12:** A vulnerability management plan is developed and implemented **RS.IM:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Section V, Step 7

Endnotes

1. For more information on the *Cyber Resilience Review*, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov
2. The *CERT-RMM* (Glossary of Terms) [Caralli 2010]
3. Caralli, R. A.; Allen, J. A.; & White, D. W. *CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1).* Addison-Wesley Professional, 2010. For more information on the CERT-RMM, please visit http://www.cert.org/resilience/products-services/cert-rmm/index.cfm.
4. Risk Steering Committee, Department of Homeland Security. *DHS Risk Lexicon – 2010 Edition.* Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf
5. *CERT-RMM*. "Controls Management" (pg. 241) [Caralli 2010].
6. *CERT-RMM*. "Vulnerability Analysis and Resolution" (pg. 915) [Caralli 2010].